(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11102333 A**

(43) Date of publication of application: **13 . 04 . 99**

(51) Int. Cl **G06F 13/00**
**G06F 13/00**
**G06F 9/06**

(21) Application number: **09260262**

(22) Date of filing: **25 . 09 . 97**

(71) Applicant: **FUJITSU LTD**

(72) Inventor: **ISHIDERA NOBUTAKA**
**SATOU SHIYUUKO**

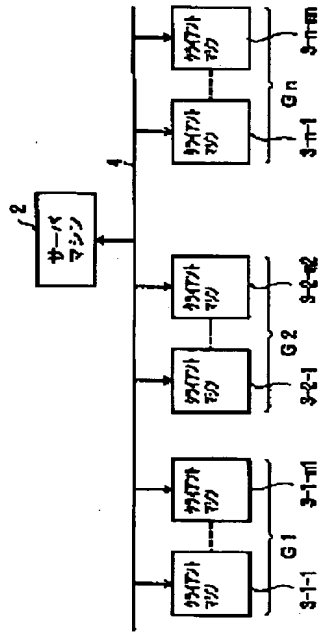
(54) **TERMINAL MANAGING METHOD, MANAGING DEVICE, AND TERMINAL DEVICE, COMPUTER SYSTEM USING THE SAME, AND RECORDING MEDIUM WHERE PROGRAM IMPLEMENTING THEM IS RECORDED**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a terminal managing method which can surely make and control a computer virus check on respective information processors connected to a network in network environment.

SOLUTION: A computer virus check request which initiates computer virus check programs of clients 3-1-1 to 3-1-m1, 3-2-1 to 3-2-m2... and 3-n-1 to 3-n-mn to is sent from a server machine to the network 4 and the clients 3-1-1 to 3-1-m1, 3-2-1 to 3-2-m2... and 3-n-1 to 3-n-mn starts the computer virus check programs at the computer virus check request from the server machine 2 to make computer virus checks.





(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－102333

(43)公開日　平成11年(1999)４月13日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 13/00 | ３５１ | Ｇ０６Ｆ | 13/00 | ３５１Ｚ |
| | | ３５４ | | | ３５４Ｚ |
| | 9/06 | ５５０ | | 9/06 | ５５０Ｚ |

審査請求　未請求　請求項の数26　ＯＬ　（全 22 頁）

(21)出願番号　特願平9－260262

(22)出願日　平成９年(1997)９月25日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　石寺　紳高
東京都稲城市大字大丸1405番地　株式会社富士通パソコンシステムズ内

(72)発明者　佐藤　周子
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　伊東　忠彦

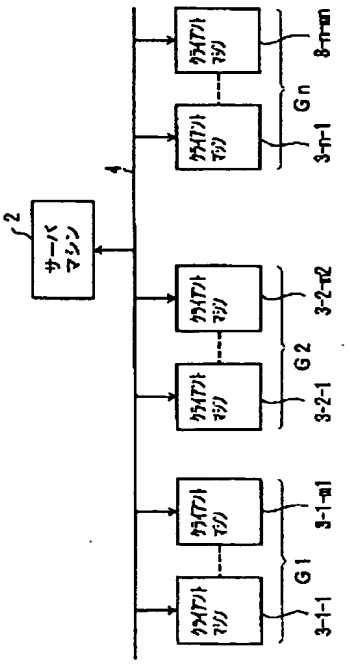
(54)【発明の名称】　端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体

(57)【要約】　（修正有）

【課題】　ネットワーク環境下でネットワークに接続された各情報処理装置のコンピュータウィルスチェックを確実に実行、管理できる端末管理方法を提供する。

【解決手段】　サーバマシン２によりクライアント３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎのコンピュータウィルスチェックプログラムを起動するコンピュータウィルスチェック要求をネットワーク４に送信し、クライアント３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎによりサーバマシン２からのコンピュータウィルスチェック要求に応じてコンピュータウィルスチェックプログラムを起動し、コンピュータウィルスチェックを実行する。

本発明の第１実施例のシステム構成図



1

【特許請求の範囲】

【請求項１】　コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置と管理装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、

前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信し、

前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動し、コンピュータウィルスチェックを実行することを特徴とする端末管理方法。

【請求項２】　前記管理装置は、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうち予め設定された所望の端末装置に供給することを特徴とする請求項１記載の端末管理方法。

【請求項３】　前記端末装置は、前記管理装置から供給される前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段で実行されたコンピュータウィルスチェック結果を前記管理装置に送信し、

前記管理装置は、前記端末装置から送信された前記コンピュータウィルスチェック結果を一括管理することを特徴とする請求項１又は２記載の端末管理方法。

【請求項４】　前記管理装置は、前記複数の端末装置から送信された前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信することを特徴とする請求項３記載の端末管理方法。

【請求項５】　前記管理装置は、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止することを特徴とすることを特徴とする請求項１乃至４のいずれか一項記載の端末管理方法。

【請求項６】　前記管理装置は、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することを特徴とする請求項１乃至５のいずれか一項記載の端末管理方法。

【請求項７】　管理装置と、複数の端末装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、

前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段を備えるとともに、コンピュータウィルスチェック要求を前記複数の端末装置に送信し、

前記複数の端末装置は、前記管理装置から送信された前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセス

2

し、自装置に対するコンピュータウィルスチェックを実行することを特徴とする端末管理方法。

【請求項８】　前記管理装置は、前記コンピュータウィルスチェック要求を前記複数の端末装置のうち予め設定された所望の端末装置に供給することを特徴とする請求項７記載の端末管理方法。

【請求項９】　前記端末装置は、前記管理装置の前記コンピュータウィルスチェック手段を起動することにより得られるコンピュータウィルスチェック結果を前記管理装置に送信し、

前記管理装置は、前記端末装置から送信されたコンピュータウィルスチェック結果を管理情報として一括管理することを特徴とする請求項７又は８記載の端末管理方法。

【請求項１０】　前記管理装置は、前記複数の端末装置から送信されたコンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信することを特徴とする請求項９記載の端末管理方法。

【請求項１１】　前記管理装置は、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止することを特徴とする請求項７乃至１０のいずれか一項記載の端末管理方法。

【請求項１２】　コンピュータウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネツトワークを介して接続される管理装置であって、

前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手段と、

前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手段とを備えることを特徴とする管理装置。

【請求項１３】　前記コンピュータウィルスチェック要求を、前記複数の端末装置のうちいずれの端末装置に送信するかを指定する指定手段を備え、

前記指定手段により指定された端末装置に対して前記コンピュータウィルスチェック要求を送信することを特徴とする請求項１２記載の管理装置。

【請求項１４】　前記送信した前記コンピュータウィルスチェック要求に応じて前記端末装置で行われたコンピュータウィルスチェック結果を受信する受信手段と、

前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を管理する管理手段とを備えることを特徴とする講求項１２または１３記載の管理装置。

【請求項１５】　前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された端末装置に送信する送信するこ

とを特徴とする請求項１４記載の管理装置。

【請求項１６】　前記複数の端末装置の接続状態を監視する監視手段と、

前記複数の端末装置のうち所定期間接続されていない端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与する情報付与手段と、

前記情報が付与された端末装置には前記コンピュータウィルスチェック要求の送信を停止する送信停止手段とを備えることを特徴とする請求項１２乃至１５のいずれか一項記載の管理装置。

【請求項１７】　前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信するコンピュータウィルスパターン送信手段を備えることを特徴とする講求項１２乃至１６のいずれか一項記載の管理装置。

【請求項１８】　ネットワークを介して管理装置に接続される端末装置であって、

前記管理装置からのコンピュータウィルスチェック要求を受信する手段と、

前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する起動手段と、コンピュータウィルスのチェックを実行するチェック実行手段とを備えることを特徴とする端末装置。

【請求項１９】　前記受信したコンピュータウィルスチェック要求に応じて実行したコンピュータウィルスチェックの結果を前記管理装置に送信する送信手段を備えることを特徴とする請求項１８記載の端末装置。

【請求項２０】前記コンピュータウィルスチェック要求とともにコンピュータウィルスパターンを受信し、該コンピュータウィルスパターンを用いてウィルスのチェックを行うことを特徴とする請求項１８または１９記載の端末装置。

【請求項２１】　ネットワークを介して管理装置に接続される端末装置であって、

前記管理装置からのコンピュータウィルスチェック要求を受信する受信手段と、

前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、自装置に対するコンピュータウィルスチェックを実行する手段とを備えることを特徴とする端末装置。

【請求項２２】　コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置と管理装置とがネットワークを介して接続されたコンピュータシステムにおいて、

前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、

前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック起動手段を備えることを特徴とするコンピュータシステム。

【請求項２３】　管理装置と複数の端末装置とがネットワークを介して接続されたコンピュータシステムにおいて、

前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段と、

コンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、

前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセスするアクセス手段と、

自装置に対するコンピュータウィルスチェックを実行するコンピュータウィルスチェック実行手段とを備えることを特徴とするコンピュータシステム。

【請求項２４】　ウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続されるコンピュータに、

前記コンピュータウイルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手順と、

前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２５】　ネットワークを介して管理装置に接続されるコンピュータに、

前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する手順と、コンピュータウィルスのチェックを実行する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２６】　ネットワークを介して管理装置に接続されるコンピュータに、

前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、該コンピュータウィルスチェック手段を起動する手順と、

前記起動されたコンピュータウィルスチェック手段により自装置に対するコンピュータウィルスチェックを実行する手順とを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

5

【発明の属する技術分野】本発明は端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体に係り、特に、ネットワークに接続された複数の端末装置をネットワークに接続された管理装置により一括して管理する端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体に関する。

【０００２】近年、情報処理装置などでは、コンピュータウィルス種の増加に伴い、ウィルスチェックは欠かすことができない。特に、ネットワーク環境においては、コンピュータウィルスへの感染はネットワーク下の全ての情報処理装置に影響があるので、定期的なコンピュータウィルスチェックが欠かせない。このため、ネットワーク環境下にネットワークに接続された端末装置（情報処理装置）のコンピュータウィルスチェックの状態をネットワーク管理者などが一括して管理している。

【０００３】しかし、各端末装置でのコンピュータウィルスチェックの実行は、人為的であり、計画的な運用管理が行えない。

【０００４】

【従来の技術】従来のネットワーク環境下の情報処理装置ではコンピュータウィルスのチェックは、各情報処理装置に記憶されたコンピュータウィルスチェックプログラムを各情報処理装置のそれぞれで、その情報処理装置を使用するユーザ自身が任意に起動することで実行されている。

【０００５】

【発明が解決しようとする課題】しかるに、従来のネットワーク環境下でのコンピュータウィルスチェック方法は、各情報処理装置にコンピュータウィルスチェックプログラムを格納しておき、各情報処理装置毎に情報処理装置の使用者がコンピュータウィルスプログラムを起動して、コンピュータウィルスチェックを行い、口頭や電子メールなどによりネットワーク管理者に報告していたため、人為的な要素が多く、ウィルスチェックを確実に行えなず、また、運用管理も容易でない等の問題点があった。

【０００６】本発明は上記の点に鑑みてなされたもので、ネットワーク環境下でネットワークに接続された各情報処理装置のコンピュータウィルスチェックを確実に実行、管理できる端末管理方法及び管理装置及び端末装置、並びに、それらを用いたコンピュータシステム及びそれらを実行するプログラムが記録された記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の請求項１は、ファイル中のコンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置

6

と該複数の端末装置のコンピュータウィルスチェックを管理する管理装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動し、コンピュータウィルスチェックを実行することを特徴とする。

【０００８】請求項１によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【０００９】請求項２は、前記管理装置を、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうち予め設定された所望の端末装置に供給する構成としてなる。請求項２によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【００１０】請求項３は、前記端末装置を、前記管理装置から供給される前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段で実行されたコンピュータウィルスチェック結果を前記管理装置に送信し、前記管理装置を、前記端末装置から送信された前記コンピュータウィルスチェック結果を一括管理する構成としてなる。

【００１１】請求項３によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。請求項４は、前記管理装置を、前記複数の端末装置から送信された前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信する構成としてなる。

【００１２】請求項４によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックでき

る。

【００１３】請求項５は、前記管理装置を、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止する構成としてなる。請求項５によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。

【００１４】請求項６は、前記管理装置を、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信する構成としてなる。請求項６によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる。

【００１５】請求項７は、ファイル中のコンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する管理装置と、該管理装置によりコンピュータウィルスチェックが管理される複数の端末装置とがネットワークを介して接続されたネットワークシステムにおける端末管理方法であって、前記管理装置は、前記コンピュータウィルスチェック要求を前記複数の端末装置に送信し、前記複数の端末装置は、前記管理装置から送信された前記コンピュータウィルスチェック要求に応じて前記管理装置に記憶された前記コンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することを特徴とする。

【００１６】請求項７によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【００１７】請求項８は、前記管理装置を、前記コンピュータウィルスチェック要求を前記複数の端末装置のうち予め設定された所望の端末装置に供給する構成としてなる。請求項８によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【００１８】請求項９は、前記端末装置を、前記管理装置から供給される前記コンピュータウィルスチェック手段を起動することにより得られるコンピュータウィルスチェック結果を前記管理装置に送信し、前記管理装置は、前記端末装置から送信されたコンピュータウィルスチェック結果を管理情報として一括管理する構成としてなる。

【００１９】請求項９によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を一括してチェックできる。請求項１０は、前記管理装置を、前記複数の端末装置から送信されたコンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された所望の端末装置に送信する構成としてなる。

【００２０】請求項１０によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる。

【００２１】請求項１１は、前記管理装置を、前記複数の端末装置のうち所定の期間接続されていない端末装置には、該端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与し、前記コンピュータウィルスチェック要求の送信を停止する構成としてなる。請求項１１によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。

【００２２】請求項１２は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続される管理装置であって、前記コンピュータウィルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手段と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手段とを備えることを特徴とする。

【００２３】請求項１２によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコン

ピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【００２４】請求項１３は、前記コンピュータウィルスチェック要求を、前記複数の端末装置のうちいずれの端末装置に送信するかを指定する指定手段を備え、前記指定手段により指定された端末装置に対して前記コンピュータウィルスチェック要求を送信することを特徴とする。請求項１３によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる。

【００２５】請求項１４は、前記送信した前記コンピュータウィルスチェック要求に応じて前記端末装置で行われたコンピュータウィルスチェック結果を受信する受信手段と、前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を管理する管理手段とを備えることを特徴とする。

【００２６】請求項１４によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。請求項１５は、前記複数の端末装置から受信した前記コンピュータウィルスチェック結果を前記複数の端末装置のうち予め設定された端末装置に送信する送信することを特徴とする。

【００２７】請求項１５によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる。

【００２８】請求項１６は、前記複数の端末装置の接続状態を監視する監視手段と、前記複数の端末装置のうち所定期間接続されていない端末装置の管理情報として、前記コンピュータウィルスチェックが行われていない旨の情報を付与する情報付与手段と、前記情報が付与された端末装置には前記コンピュータウィルスチェック要求の送信を停止する送信停止手段とを備えることを特徴とする。

【００２９】請求項１６によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる。請求項１７は、前記端末装置に前記コンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信するコンピュータウィルスパターン送信手段を備えることを特徴とする。

【００３０】請求項１７によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる。

【００３１】請求項１８は、ネットワークを介して管理装置に接続される端末装置であって、前記管理装置からのコンピュータウィルスチェック要求を受信する手段と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する起動手段と、コンピュータウィルスのチェックを実行するチェック実行手段とを備えることを特徴とする。

【００３２】請求項１８によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【００３３】請求項１９は、前記受信したコンピュータウィルスチェック要求に応じて実行したコンピュータウィルスチェックの結果を前記管理装置に送信する送信手段を備えることを特徴とする。請求項１９によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる。

【００３４】請求項２０は、前記コンピュータウィルスチェック要求とともにコンピュータウィルスパターンを受信し、該コンピュータウィルスパターンを用いてウィルスのチェックを行うことを特徴とする。請求項２０によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィ

ルスチェックを行うことができる。

【００３５】請求項２１は、ネットワークを介して管理装置に接続される端末装置であって、前記管理装置からのコンピュータウィルスチェック要求を受信する受信手段と、前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、自装置に対するコンピュータウィルスチェックを実行する手段とを備えることを特徴とする。

【００３６】請求項２１によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【００３７】請求項２２は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段を具備する複数の端末装置と管理装置とがネットワークを介して接続されたコンピュータシステムにおいて、前記管理装置は、前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、前記複数の端宋装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記コンピュータウィルスチェック手段を起動するコンピュータウィルスチェック起動手段を備えることを特徴とする。

【００３８】請求項２２によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【００３９】請求項２３は、管理装置と複数の端末装置とがネットワークを介して接続されたコンピュータシステムにおいて、前記管理装置は、コンピュータウィルスをチェックするコンピュータウィルスチェック手段と、コンピュータウィルスチェック要求を前記複数の端末装置に送信するコンピュータウィルスチェック要求送信手段を備え、前記複数の端末装置は、前記管理装置からの前記コンピュータウィルスチェック要求に応じて前記管理装置の前記コンピュータウィルスチェック手段にアクセスするアクセス手段と、自装置に対するコンピュータウィルスチェックを実行するコンピュータウィルスチェック実行手段とを備えることを特徴とする。

【００４０】請求項２３によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【００４１】請求項２４は、ウィルスをチェックするコンピュータウィルスチェック手段をそれぞれ具備する複数の端末装置とネットワークを介して接続されるコンピュータに、前記コンピュータウイルスチェック手段を起動させるコンピュータウィルスチェック要求を生成する手順と、前記生成したコンピュータウィルスチェック要求を前記複数の端末装置にそれぞれ送信する手順とを実行させるためのプログラムを記録媒体に記録することを特徴とする。

【００４２】請求項２４によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【００４３】請求項２５は、ネットワークを介して管理装置に接続されるコンピュータに、前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、前記コンピュータウィルスチェック要求の受信に応じてコンピュータウィルスチェックを起動する手順と、コンピュータウィルスのチェックを実行する手順とを実行させるためのプログラムをコンピュータ読み取り可能な記録媒体に記録したことを特徴とする。

【００４４】請求項２５によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる。

【００４５】請求項２６は、ネットワークを介して管理装置に接続されるコンピュータに、前記管理装置からのコンピュータウィルスチェック要求を受信する手順と、

前記コンピュータウィルスチェック要求の受信に応じて前記管理装置のコンピュータウィルスチェック手段にアクセスし、該コンピュータウィルスチェック手段を起動する手順と、前記起動されたコンピュータウィルスチェック手段により自装置に対するコンピュータウィルスチェックを実行する手順とを実行させるためのプログラムをコンピュータ読み取り可能な記録媒体に記録したことを特徴とする。

【００４６】請求項２６によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる。

【００４７】

【発明の実施の形態】図１に本発明の第１実施例のシステム構成図を示す。本実施例のネットワークシステム１は、サーバマシン２とクライアントマシン３－１－１～３－ｎ－ｍとがネットワーク４を介して接続されている。ここで、まず、サーバマシン２の構成を図面とともに説明する。

【００４８】図２に本発明の第１実施例のサーバマシンのブロック構成図を示す。サーバマシン２は、ネットワーク４との通信を制御する通信制御部１１、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎに供給すべき情報等がファイルされたファイル装置１２、ファイル装置１２に情報を書き込むとともにファイル装置１２から情報を読み出す制御を行う入出力コントローラ１３、ファイル装置１２のプログラム領域に格納されたコンピュータウィルスチェック要求プログラムに応じて処理を実行するＣＰＵ１４、ＣＰＵ１４の作業領域となるＲＡＭ１５、処理結果を表示するディスプレイ１６、ディスプレイ１６を制御する表示コントローラ１７、コマンド、データを入力するキーボード１８、キーボード１８の入力を制御するキーボードコントローラ１９、通信制御部１１、入出力コントローラ１３、ＣＰＵ１４、ＲＡＭ１５、表示コントローラ１７、キーボードコントローラ１９を接続するバス２０から構成される。

【００４９】通信制御部１１はネットワーク２に接続され、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎとの接続を行う。ファイル装置１２は、データが格納されるデータ領域１２ａ、サーバマシン２で実行されるプログラムが格納されたプログラム領域１２ｂ、コンピュータウィルスチェック要求プログラム実行時のタイミングを制御するデータが格納されたコンピュータウィルスチェック要求スケジュール領域１２ｃ、コンピュータウィルスチェック結果処理プログラム実行時にクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎから供給されたコンピュータウィルスチェック結果を保持する結果累積領域１２ｄから構成される。

【００５０】上記のコンピュータウィルスチェック要求プログラム、コンピュータウィルスチェック結果処理プログラムなどのプログラムやデータは、通信制御部を介して、または図示しないＣＤ－ＲＯＭやフロッピィディスクなどの可搬型記録媒体に記録されたものを読取装置を用いて読み取られ、上記ファイル装置１２のプログラム領域１２ａやスケジュール領域１２ｃに格納される。そして、それらはプログラムの実行時に作業領域であるＲＡＭ１５に格納され、ＣＰＵ１４はそれらプログラムに応じて所定の処理を実行する。

【００５１】図３に本発明の第１実施例のコンピュータウィルスチェック要求スケジュールのデータ構成図を示す。サーバマシン２は、クライアントマシン３－１－１～３－ｎ－ｍｎを複数のグループＧ１～Ｇｎに分割して管理している。ここで、図１に示すようにグループＧ１は、クライアントマシン３－１－１～３－１－ｍ１、グループＧ２は、クライアントマシン３－２－１～３－２－ｍ２・・・、グループＧｎは、クライアントマシン３－ｎ－１～３－ｎ－ｍｎから構成される。

【００５２】コンピュータウィルスチェック要求スケジュール領域１２ｃは、グループＧ１～Ｇｎ毎に設定される。１グループ分のコンピュータウィルスチェック要求スケジュール１２ｃは、主に、スケジュールを設定するグループＧ１～Ｇｎの情報を示すグループ情報ヘッダ領域、グループ情報ヘッダ領域で設定されたグループに属するメンバ（クライアントマシン）の情報を示すメンバ情報領域、１グループの情報の終了を示すグループ情報エンダ領域から構成される。

【００５３】また、グループ情報ヘッダ領域は、スケジュールを設定するグループＧ１～Ｇｎを識別するためのグループＩＤ領域、コンピュータウィルスチェック要求を発行すべき日時を設定するための発行日時情報領域、グループの管理者のメールアドレスを示す管理者メールアドレス領域、グループに属するクライアントマシンの数が設定されるメンバ数領域、コンピュータウィルスチェックに用いられるコンピュータウィルスチェックプログラムのバージョンを示すバージョン情報領域から構成される。

【００５４】また、メンバ情報領域は、コンピュータウイルスチェックを行うクライアントマシンを識別するためのメンバＩＤ領域、コンピュータウイルスチェックを

行うクライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn を使用する人の名前などを設定するメンバ名、コンピュータウイルスチェックを行うクライアントマシンを使用する人のメールアドレスを設定するメンバメールアドレス領域、コンピュータウイルスのチェック結果を通知する先のアドレスを設定するための結果通知先アドレス領域、１メンバ情報の終了を示すエンダ領域から構成される。上記メンバ情報領域がメンバ数分だけ繰り返され、最後にエンダが付与されて、１グループ情報領域とされる。

【００５５】サーバマシン２は、上記チェック要求スケジュール１２ｃを監視しており、現在時刻がチェック要求スケジュール管理１２ｃの発行日時情報領域に設定された発行日時になったとき、後述するようにチェック要求スケジュール１２ｃに設定された情報に基づいてコンピュータウィルスチェックの要求を行う。図４に本発明の第１実施例の集計結果累積領域のデータ構成図を示す。

【００５６】集計結果累積領域１２ｄは、クライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn を識別するためのメンバＩＤが格納されるメンバＩＤ領域、メンバＩＤ領域に格納されたメンバＩＤを使用する人に名前などのメンバ名が格納されるメンバ名領域、メンバＩＤ領域に格納されたメンバＩＤのクライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn でのコンピュータウィルスチェック結果、及び、コンピュータウィルスチェックに用いられたコンピュータウィルスチェックプログラムのバージョン情報が格納される結果格納領域から１メンバ分の情報が構成される。集計結果累積領域１２ｄは、上記メンバＩＤ領域、メンバ名領域、結果格納領域がメンバ数だけ繰り返される。

【００５７】サーバマシン２は、コンピュータウィルスチェック要求プログラムによりファイル装置１２のコンピュータウィルスチェック要求スケジュール領域１２ｃに予め設定されたスケジュールに応じてクライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn にコンピュータウィルスチェック要求を送信し、コンピュータウィルスチェック結果処理プログラムによりクライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn でのコンピュータウィルスチェック結果を集計して、管理者に送信する。

【００５８】次にクライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn の構成を図面とともに説明する。図５に本発明の第１実施例のクライアントマシンのブロック構成図を示す。クライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn は、ネットワーク４との通信を制御する通信制御部２１、データ、プログラムなどが格納されるファイル装置２２、ファイル装置２２に情報を書き込むとともにファイル装置２２から情報を読み出す制御を行う入出力コントローラ２３、ファイル装置２２のプログラム領域に格納されたコンピュータウィルスチェックプログラムに応じてコンピュータウィルスチェックを実行するＣＰＵ２４、ＣＰＵ２４の作業領域となるＲＡＭ２５、処理結果を表示するディスプレイ２６、ディスプレイ２６を制御する表示コントローラ２７、コマンド、データを入力するキーボード２８、キーボード２８の入力を制御するキーボードコントローラ２９、通信制御部２１、入出力コントローラ２３、ＣＰＵ２４、ＲＡＭ２５、表示コントローラ２７、キーボードコントローラ２９を接続するバス３０から構成される。

【００５９】通信制御部２１はネットワーク２に接続され、サーバマシン２との接続を制御する。ファイル装置２２は、データが格納されるデータ領域２２ａ、クライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn で実行されるプログラムが格納されたプログラム領域２２ｂ、コンピュータウィルスチェック結果を格納するコンピュータウィルスチェック結果格納領域２２ｃ、コンピュータウィルスチェックプログラム実行時に用いられるコンピュータウィルスパターン領域２２ｄから構成される。

【００６０】上記のコンピュータウイルスチェックプログラムなどの本発明に関わるプログラムやウィルスパターンは、通信制御部を介して、または図示しないＣＤ－ＲＯＭやフロッピィディスクなどの可搬型記録媒体に記録されてたものを読取装置を用いて読み取られ、上記ファイル装置２２のプログラム領域２２ｂやコンピュータウィルスパターン領域２２ｄに格納される。そして、それらはプログラムの実行時に作業領域であるＲＡＭ２５に格納され、ＣＰＵ２４はそれらプログラムに応じて所定の処理が実行される。

【００６１】図６に本発明の第１実施例のクライアントマシンのコンピュータウィルスチェック結果領域のデータ構成図を示す。クライアントマシン３－１－１～３－１－ml，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn では、コンピュータウィルスチェックプログラムによるコンピュータウィルスチェック結果を図６に示すようなデータ形式のコンピュータウィルスチェック結果格納領域２２ｃに格納した後、サーバ２に送信する。

【００６２】まず、コンピュータウィルスチェック結果格納領域２２ｃは、自装置の属するグループを認識するためのグループＩＤが格納されるグループＩＤ領域、自装置を認識するためのメンバＩＤが格納されるメンバＩＤ領域、ステップＳ２－２でのコンピュータウィルスチ

ェック結果を格納するための結果領域、コンピュータウィルスチェックプログラムで使用したコンピュータウィルスパターンのバージョン情報を格納するためのバージョン情報領域から構成される。

【００６３】図７に本発明の第１実施例のクライアントマシンのコンピュータウィルスパターン領域のデータ構成図を示す。クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎのファイル装置２２に設定されたコンピュータウィルスパターンファイル領域２２ｄは、バージョンを識別するためのバージョン情報が格納されたバージョン情報領域、バージョン情報に応じたコンピュータウィルスのパターンが格納されるコンピュータウィルスパターン領域とから構成される。

【００６４】クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎでは、サーバマシン２から供給される自装置へのコンピュータウィルスチェック要求に応じてコンピュータウィルスチェックプログラムが起動し、ファイル装置２２に設定されたコンピュータウィルスパターンファイル領域２２ｄのコンピュータウィルスパターンを参照し、ファイル装置２２のデータ領域２２ａ、及び、プログラム領域２２ｂに格納されたデータとコンピュータウィルスパターンファイル領域２２ｄのコンピュータウィルスパターンと比較して、一致するパターンを検索し、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行う。

【００６５】次に、サーバマシン２で実行されるコンピュータウィルス要求プログラムの動作を図面と共に説明する。図８に本発明の第１実施例のサーバマシンのコンピュータウィルスチェック要求プログラムの処理フローチャートを示す。サーバマシン２では、コンピュータウィルス要求プログラムにより、まず、図３に示す要求スケジュールを参照して、設定されているメンバ情報を順次取り出す（ステップＳ１－１，Ｓ１－２，Ｓ１－３）。

【００６６】次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する（ステップＳ１－４）。ステップＳ１－４の比較結果、発行日時が現在日時であれば、メンバ情報領域を順に読み出し、各メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットをネットワーク４に送信する（ステップＳ１－５，Ｓ１－６）。

【００６７】クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎは、ネットワーク４上のパケット監視しており、自装置のパケットのみを受信する。次に、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎのコンピュータウィルスチェックプログラムの動作を図面と共に説明する。

【００６８】図９に本発明の第１実施例のクライアントマシンのコンピュータウィルスチェックプログラムの処理フローチャートを示す。クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎではサーバマシン２から自装置宛のコンピュータウィルスチェック要求パケットを受信すると、コンピュータウィルスチェックプログラムを起動させる（ステップＳ２－１）。

【００６９】ステップＳ２－１でコンピュータウィルスチェックプログラムが起動されると、ファイル装置２２のデータ領域２２ａ及びプログラム領域２２ｂに格納されたデータを順次読み出し、コンピュータウィルスパターン領域２２ｄのコンピュータウィルスパターンと比較して一致するパターンを検索する。比較結果、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行うとともに、コンピュータウィルスパターンのバージョン情報、及び、検出したウィルスの情報を保持する。また、比較結果、コンピュータウィルスパターンと一致するデータが存在しない場合には、ウィルスは存在しないと判断して、チェックしたコンピュータウィルスパターンのバージョン情報、及び、ウィルスが存在しない旨の情報を保持する。

【００７０】次に、コンピュータウィルスチェックプログラムのチェック結果をサーバへの報告形式にまとめ、ファイル装置２２のコンピュータウィルスチェック結果領域２２ｃに格納する（ステップＳ２－２）。クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎは、ステップＳ２－２でのコンピュータウィルスチェックプログラムによるコンピュータウィルスのチェック後、図６に示すように自装置の属するグループＩＤ、自装置のメンバＩＤ、ウィルスチェック結果、コンピュータウィルスパターンのバージョン情報からなる結果報告情報を含むサーバマシン２宛のパケットを作成して、サーバマシン２に通知する（ステップＳ２－３）。

【００７１】サーバマシン２は、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎからコンピュータウィルスのチェック結果を受信すると、コンピュータウィルスチェック結果処理プログラムを実施する。次に、サーバマシン２のコンピュータウィルスチェック結果処理プログラムの動作を図面とともに説明する。

【００７２】図１０に本発明の第１実施例のサーバマシンのコンピュータウィルスチェック結果処理プログラムの処理フローチャートを示す。サーバマシン２では、クライアントマシン３－１－１～３－１－ｍ１，３－２－

１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn からコンピュータウィルスのチェック結果パケットを受信すると、コンピュータウィルスチェック結果プログラムが起動し、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn から受信したコンピュータウィルスチェック結果をグループ毎にファイル装置１２の集計結果累積領域１２ｄに保存する（ステップＳ３－１）。

【００７３】ステップＳ３－１でコンピュータウィルスチェック結果を保存する際の情報は、グループ毎に保存される。１グループの情報は、図４に示す１メンバの情報が繰り返し、メンバ分だけ順次配列された構成とされている。１メンバ分の情報は、メンバ名、コンピュータウィルスチェック結果、ウィルスチェックパターンのバージョン情報から構成され、これがメンバ数分だけ繰り返したファイルとして保存される。このとき、ファイル名を、例えば、グループＩＤ及びコンピュータウィルスチェック日時をアンダーバー記号を介して配列し、ファイル形式（拡張子）を付与したものとすることにより、ファイル名から容易にグループ及びコンピュータウィルスチェック日時を認識できる。

【００７４】図６に示すようにクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn からのコンピュータウィルスチェック結果が保存されると、次に、処理結果をコンピュータウィルスチェック要求スケジュール１２ｃのメンバ情報領域の結果通知先アドレス領域に格納されたアドレス宛に送信する（ステップＳ３－２）。

【００７５】ステップＳ３－２でグループ内の全てのクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のコンピュータウィルスチェック結果が得られると、次に、保存されたコンピュータウィルスの処理結果でグループ内の全てのクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn からコンピュータウィルスチェック結果が得られていれば（ステップＳ３－３）、次に、同じグループ内の全てのクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のコンピュータウィルスチェック結果を一覧にし、図３に示されるコンピュータウィルスチェック要求スケジュール１２ｃのグループ情報ヘッダ領域の管理者メールアドレス領域に格納された管理者メールアドレス宛に送信する（ステップＳ３－４）。

【００７６】図１１に本発明の第１実施例のグループ担当者（管理者）に送信するコンピュータウィルスチェック結果一覧のフォーマットを示す。ステップＳ３－４では、図４に示す集計結果累積領域１２ｄに格納されたクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のコンピュータウィルスチェック結果からグループ担当者に送信するコンピュータウィルスチェック結果一覧をテキストファイル形式で作成し、管理者に送信する。コンピュータウィルスチェック結果一覧は、図１１に示すように、最上段に、グループＩＤ、及び、コンピュータウィルスチェックが実施された日時が記録される。図１１では、グループＩＤが「Ａ」、施行日時が「９７年７月７日」であることがわかる。

【００７７】次の段から順次グループに属するクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn でのコンピュータウィルスチェック結果が記録される。コンピュータウィルスチェック結果を記録する領域には、メンバ名、バージョン情報、コンピュータウィルスチェック結果が記録される。

【００７８】図１１の上段に記録された領域には、メンバ名「Ａ氏」、バージョン情報「Ｖ＊＊Ｌ＊＊」であり、コンピュータウィルスチェック結果はコンピュータウィルスが発見できない状態である情報「Normal end」が記録されている。また、図１１の下段に記録された領域には、メンバ名「Ｂ氏」、バージョン情報「Ｖ＊＊Ｌ＊＊」であり、コンピュータウィルスチェック結果はコンピュータウィルス「＊＊」が発見され、除去されたことを示す旨の情報が記録される。図１１に示すような情報がテキストファイルとして供給される。

【００７９】管理者は、図１１に示すようなコンピュータウィルスチェック結果一覧を参照して、自分の管理するグループのコンピュータウィルスチェックの結果を認識する。ステップＳ３－４で、図１１に示すようなコンピュータウィルスチェック結果一覧が管理者に送信された後、結果をバックアップとしてファイル装置の結果累積領域に保存する（ステップＳ３－５）。

【００８０】本実施例によれば、ネットワーク４に接続されたクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mnのコンピュータウィルスチェックをサーバ２からの要求により自動で実施できるので、コンピュータウィルスチェックを確実に実施できる。また、コンピュータウィルスチェックは、予め設定されたスケジュールに応じて実施されるため、使用時間を避けて、実際の作業を妨害することなく実施できる。さらに、定期的に実施できるので、有効なコンピュータウィルスチェックを実現できる。

【００８１】なお、本実施例では、各クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn にコンピュータウィルスチェックプログラムを搭載したが、コンピュータウィルスパターンは年々増加しており、本実施例の構成ではコンピュータウィルスパターンを更新する場合には、各クライアントマシーン３－１－１～３－１－m1，３

－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn の夫々で最新コンピュータウィルスパターンをインストールする必要があり、手間がかかる。また、各クライアントマシーン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のうち、一つのクライアントマシンでも最新コンピュータウィルスパターンのインストールを怠ると、コンピュータウィルスパターンに抜けが生じ、最新のコンピュータウィルスパターンを見逃してしまう。

【００８２】そこで、コンピュータウィルスパターンをサーバマシンから供給する構成が考えられる。第２実施例として、コンピュータウィルスパターンをサーバマシンから供給する構成の実施例について説明する。なお、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn の構成及び動作は第１実施例と同じため、その説明は省略する。

【００８３】まず、本実施例のサーバマシン５０の構成を図面とともに説明する。図１２に本発明の第２実施例のサーバマシンのブロック構成図を示す。同図中、図２と同一構成部分には同一符号を付し、その説明は省略する。本実施例のサーバマシン５０は、ファイル装置５１のデータ領域５２に最新コンピュータウィルスパターンデータ領域５２ａを有する。最新コンピュータウィルスパターンデータ領域５２ａには、最新のコンピュータウィルスパターンが格納されている。

【００８４】サーバマシン５０は、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn にコンピュータウィルスチェック要求スケジュール１２ｃに基づいて供給するコンピュータウィルスチェック要求の送信時に、コンピュータウィルスチェック要求スケジュール１２ｃに格納された各クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のコンピュータウィルスパターンのバージョン情報を参照して、最新コンピュータウィルスパターンデータ領域５２ａに格納された最新コンピュータウィルスパターンのバージョン情報と比較し、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn のコンピュータウィルスパターンに不足するコンピュータウィルスパターンをコンピュータウィルスチェック要求とともにクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn に送信する。

【００８５】図１３に本発明の第２実施例のサーバマシンのコンピュータウィルスチェック要求プログラムの処理フローチャートである。サーバマシン２では、コンピュータウィルス要求プログラムにより、まず、図３に示す要求スケジュールを参照して、設定されているメンバ情報を順次取り出す（ステップＳ４－１，Ｓ４－２，Ｓ４－３）。

【００８６】次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する（ステップＳ４－４）。ステップＳ４－４の比較結果、発行日時が現在日時であれば（ステップＳ４－５）、次に、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報を参照して、サーバマシン２のファイル装置５１のデータ領域５２に格納されたコンピュータウィルスパターンデータ５２ａのバージョン情報と比較する（ステップＳ４－６）。

【００８７】ステップＳ４－６で、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報とサーバマシン２のファイル装置５１のデータ領域５２に格納されたコンピュータウィルスパターンデータ５２ａのバージョン情報とが不一致の場合には、ウィルスチェック要求パケットにコンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのコンピュータウィルスパターンに不足するコンピュータウィルスパターン及びバージョン情報を付与して、メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットをネットワーク４に送信する（ステップＳ４－７）。

【００８８】また、ステップＳ４－６で、コンピュータウィルスチェック要求を行うクライアントマシンのメンバ情報領域に格納されたコンピュータウィルスチェックプログラムのバージョン情報とサーバマシン２のファイル装置５１のデータ領域５２に格納されたコンピュータウィルスパターンデータ５２ａのバージョン情報とが一致する場合には、メンバ情報領域のメンバメールアドレス領域に格納されたメンバメールアドレス宛にウィルスチェック要求パケットだけをネットワーク４を介して送信する（ステップＳ４－８）。

【００８９】クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn は、ネットワーク４上のパケット監視しており、自装置のパケットのみを受信する。このとき、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－ｎ－１～３－ｎ－mn は、コンピュータウィルスパターンが付与されたコンピュータウィルスチェック要求を受信すると、付与されたコンピュータウィルスパターンをコンピュータウィルスチェックプログラムのコンピュータウィルスパターンに付加するとともに、バージョン情報をコンピュータウィルスチェック要求に付与されたバージョン情報に更新する。

【００９０】以下、第１実施例の図９に示すコンピュータウィルスチェックプログラムを実行して、サーバマシン２にコンピュータウィルスチェック結果を送信する。サーバマシン２は、第１実施例の図１０に示すコンピュータウィルスチェック結果処理プログラムを実行する。本実施例によれば、クライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－n－１～３－n－mn に格納されたコンピュータウィルスチェックプログラムを常に最新のバージョンのコンピュータウィルスパターンで実行できるので、コンピュータウィルスから確実にシステムを防御できる。

【００９１】なお、本実施例では、サーバマシン５０からコンピュータウィルスパターンだけを提供する構成としたが、サーバマシンにコンピュータウィルスチェックプログラムを搭載し、コンピュータウィルスチェック時にクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－n－１～３－n－mn からアクセスする構成も考えられる。

【００９２】第３実施例として、サーバマシン２にコンピュータウィルスチェックプログラムを搭載し、コンピュータウィルスチェック時にクライアントマシン３－１－１～３－１－m1，３－２－１～３－２－m2 ・・・３－n－１～３－n－mn からアクセスする実施例について図面とともに説明する。まず、サーバマシンの構成を図面とともに説明する。

【００９３】図１４に本発明の第３実施例のサーバマシンのブロック構成図を示す。同図中、図２と同一構成部分には同一符号を付し、その説明は省略する。本実施例のサーバマシン１１０は、ファイル装置１１１のプログラム領域１１２にコンピュータウィルスをチェックするコンピュータウィルスチェックプログラムが格納されている。

【００９４】サーバマシン１１０での処理は、サーバマシンからクライアントマシンにコンピュータウィルスチェック要求を送信するまでの処理、すなわち、図８に示すコンピュータウィルスチェック要求プログラム、及び、図１０に示すクライアントマシンから供給されたコンピュータウィルスチェック結果を集計するコンピュータウィルスチェック結果処理プログラムは、第１実施例と同一である。よって、図８に示すコンピュータウィルスチェック要求プログラム及び図１０に示すコンピュータウィルスチェック結果処理プログラムの説明は省略する。

【００９５】クライアントマシン１２０は、サーバマシンからのコンピュータウィルスチェック要求に応じてサーバマシン１１０のファイル装置１１１のプログラム領域１１２に格納されたコンピュータウィルスチェックプログラムにアクセスする。次に、本実施例のクライアントマシン１２０の構成を図面とともに説明する。図１５に本発明の第３実施例のクライアントマシンのブロック構成図を示す。同図中、図５と同一構成部分には同一符号を付し、その説明は省略する。

【００９６】本実施例のクライアントマシン１２０では、ファイル装置１２１のプログラム領域１２２には、コンピュータウィルスチェックプログラムが保存されおらず、コンピュータチェック制御プログラムが保存されている。なお、上記のコンピュータウィルス制御チェックプログラムも他の実施例と同様、通信制御部を介して、または図示しないＣＤ－ＲＯＭやフロッピィディスクなどの可搬型記録媒体に記録されてたものを読取装置を用いて読み取られ、上記ファイル装置１２１のプログラム領域１２２に格納されるものであり、プログラムの実行時には作業領域であるＲＡＭ２５に格納され、そのプログラムに応じてＣＰＵ２４により所定の処理が実行されるものである。

【００９７】図１６に本発明の第３実施例のクライアントマシンのコンピュータウィルスチェック制御プログラムの処理フローチャートを示す。クライアントマシン１２０ではサーバマシン１１０から自装置へのコンピュータウィルスチェック要求パケットを受信すると、コンピュータウィルスチェック制御プログラムを起動させ、サーバマシン１１０のファイル装置１１１のプログラム領域１１２に設定されたコンピュータウィルスチェックプログラムにアクセスし、コンピュータウィルスチェックプログラムを起動させる。（ステップＳ５－１）。

【００９８】ステップＳ５－１で、サーバマシン１１０上のコンピュータウィルスチェックプログラムが起動されると、ファイル装置１２１のデータ領域２２ａに格納されたデータを順次、コンピュータウィルスパターン領域２２ｄに格納されたコンピュータウィルスパターンと比較して一致するパターンを検索する。比較結果、コンピュータウィルスパターンと一致するデータが存在する場合には、ウィルスが存在すると判断して、ウィルスパターンの除去などを行うとともに、コンピュータウィルスパターンのバージョン情報、及び、検出したウィルスの情報を保持する。また、比較結果、コンピュータウィルスパターンと一致するデータが存在しない場合には、ウィルスは存在しないと判断して、チェックしたコンピュータウィルスパターンのバージョン情報、及び、ウィルスが存在しない旨の情報を保持する。

【００９９】次に、コンピュータウィルスチェックプログラムのチェック結果を図６に示すようなサーバへの報告形式にまとめる（ステップＳ５－２）。クライアントマシン１２０は、ステップＳ５－２でのサーバマシンに記憶されたコンピュータウィルスチェックプログラムによるコンピュータウィルスのチェック後、図６に示すように自装置の属するグループＩＤ、自装置のメンバＩＤ、ウィルスチェック結果、コンピュータウィルスパターンのバージョン情報からなる結果報告情報を含むパケットを作成して、サーバマシンに通知する（ステップＳ

５－３）。

【０１００】サーバマシン１１０は、クライアントマシン１２０からコンピュータウィルスのチェック結果を受信すると、図１０に示すようにコンピュータウィルスチェック結果処理プログラムを実施する。本実施例によれば、サーバマシン１１０にコンピュータウィルスチェックプログラムを持ち、サーバマシン１１０からのコンピュータウィルスチェック要求に対してクライアントマシン１２０がサーバマシン１１０のコンピュータウィルスチェックプログラムにアクセスすることによりコンピュータウィルスのチェックを行うことにより、クライアントマシン１２０を全て同一バージョンのコンピュータウィルスパターンでチェックでき、サーバマシン１１０のコンピュータウィルスパターンを最新のバージョンにしておくだけで、全てのクライアントマシン１２０を最新のバージョンのコンピュータウィルスパターンでチェックできるので、クライアントマシン１２０をコンピュータウィルスから確実に防御できる。

【０１０１】また、クライアントマシン１２０は、コンピュータウィルスチェックプログラムを記憶する必要がないので、有効に使えるファイル領域が増大させることができる。なお、第１及び第３実施例では、サーバマシンはクライアントマシンの接続状態によらず、無条件にコンピュータウィルスチェック要求を行っていいたが、所定の条件に従ってコンピュータウィルスチェック要求を行うことにより処理の自由度を向上させることもできる。

【０１０２】次に、所定の条件に従ってコンピュータウィルスチェック要求を行う実施例について説明する。まず、本実施例のサーバマシン１１０の構成を図面とともに説明する。図１７に本発明の第４実施例のサーバマシンのブロック構成図を示す。同図中、図２と同一構成部分には同一符号を付し、その説明は省略する。

【０１０３】本実施例のサーバマシン２１０は、ファイル装置２１１に発信状況管理領域２１２を有する。発信状況管理領域２１２には、サーバマシン２１０でコンピュータウィルスチェックを行うクライアントマシンのコンピュータウィルスチェック要求発信予定日、各クライアントマシンを有効とする期限などを一括して管理する情報が格納される。

【０１０４】なお、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０と同一であるのでその説明は省略する。図１８に本発明の第４実施例のサーバマシンの発信状況管理領域のデータ構成図を示す。

【０１０５】発信状況管理領域２１２は、サーバマシン２１０からのコンピュータウィルスチェックが有効となるクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０が属するグループＩＤを格納するグループＩＤ領域、クライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０のメンバＩＤを格納するメンバＩＤ領域、設定されたクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０のコンピュータウィルスチェック結果を送信する先のメールアドレスを格納するメールアドレス領域、コンピュータウィルスチェック要求の発信予定日を格納する発信予定日領域、コンピュータウィルスチェック要求を発信する期限を格納する発信期限領域から構成される。発信状況管理領域には、上記の情報を有効とするクライアントマシン数分だけ繰り返して格納される。

【０１０６】サーバマシン２１０は、図１８に示す発信状況管理領域の情報に基づいてクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０にコンピュータウィルスチェック要求を発信する。図１９に本発明の第４実施例のサーバマシンのコンピュータウィルスチェック要求処理プログラムの処理フローチャートを示す。

【０１０７】サーバマシン２１０では、コンピュータウィルス管理プログラムにより、図６に示すような要求スケジュールの参照して、設定されているグループ情報を順次取り出す（ステップＳ６－１，Ｓ６－２，Ｓ６－３）。次に、グループ情報中の発行日時情報領域に格納された発行日時情報を読み出して、現在日時と比較する（ステップＳ６－４）。ステップＳ６－４の比較結果、発行日時が現在日時であれば、要求スケジュールから参照したメンバ情報を読み出し、発信情報管理領域の対応する領域に設定する（ステップＳ６－５、Ｓ６－６）。

【０１０８】要求スケジュールをチェックし終わると（ステップＳ６－３）、次に、ステップＳ６－６で順次情報が設定された発信情報管理領域の情報を順次最終の情報まで参照する（ステップＳ６－７，Ｓ６－８）。このとき、まず、発信情報管理領域の期限領域に格納された期限を参照し、コンピュータウィルスチェックを行う期限が切れているか否かを判定する（ステップＳ６－９）。ステップＳ６－９での判定結果、コンピュータウィルスチェックを行う期限が切れている場合には、発信情報管理領域からそのメンバ情報を削除し、また、結果累積領域の対応するメンバ情報に期限切れである旨の情報を記録し、ステップＳ６－７に戻って、次のメンバ情報を参照する（ステップＳ６－１０）。

【０１０９】また、ステップＳ６－９での判定結果、コンピュータウィルスチェックを行う期限が有効である場合には、次に、現在参照しているメンバ情報のクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０にアクセスし、クライアントマシン３－１－１～

３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０の接続状態を検出する（ステップＳ６－１１）。

【０１１０】ステップＳ６－１１での検出結果、現在参照しているクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０が接続されていなければ、ステップＳ６－７に戻って、次のメンバ情報を参照する。また、ステップＳ６－１１での検出結果、現在参照しているクライアントマシン３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ、または、１２０が接続されていれば、コンピュータウィルスチェックを行うべきクライアントマシンであると判断できるので、発信情報管理領域の現在参照しているメンバ情報に設定されたメンバＩＤにコンピュータウィルスチェックを行う要求を行うためのコンピュータウィルスチェック要求パケットを送信し、発信情報管理領域の現在参照しているメンバ情報を削除して、ステップＳ６－７に戻って、次のメンバ情報を参照する（ステップＳ６－１２）。

【０１１１】本実施例によれば、電源の切断、故障などによりサーバマシン２１０から接続できない、または、有効期限が切れて接続すべきでないクライアントマシンを判定して、「不在」として要求をスキップして、自動でコンピュータウィルスチェックを実行できる。

【０１１２】

【発明の効果】上述の如く、本発明の請求項１によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１１３】請求項２によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【０１１４】請求項３によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項４によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【０１１５】請求項５によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【０１１６】請求項６によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行でき、また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができ、最新のウィルスパターンへの更新が容易に行える等の特長を有する。

【０１１７】請求項７によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【０１１８】請求項８によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【０１１９】請求項９によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を一括してチェックできる等の特長を有する。請求項１０によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック

結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【０１２０】請求項１１によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【０１２１】請求項１２によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１２２】請求項１３によれば、管理装置によりコンピュータウィルスチェック要求を複数の端末装置のうち予め設定された所望の端末装置に供給することにより、コンピュータウィルスチェックを行わせたい端末装置だけで、コンピュータウィルスチェックを行わせることができるため、複数の端末装置を複数のグループに分割して、グループ毎にコンピュータウィルスチェックを実行できる等の特長を有する。

【０１２３】請求項１４によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項１５によれば、複数の端末装置から送信されたコンピュータウィルスチェック結果を複数の端末装置のうち予め設定された所望の端末装置に送信することにより、管理装置のみならず、所望の端末装置からコンピュータウィルスチェック結果を出力し、複数の端末装置のコンピュータウィルスへの感染をチェックできる等の特長を有する。

【０１２４】請求項１６によれば、複数の端末装置のうち所定の期間接続されていない端末装置には、端末装置の管理情報として、コンピュータウィルスチェックが行われていない旨の情報を付与し、コンピュータウィルスチェック要求の送信を停止することにより、不要なコンピュータウィルスチェック要求を低減できる等の特長を有する。

【０１２５】請求項１７によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる等の特長を有する。

【０１２６】請求項１８によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１２７】請求項１９によれば、端末装置でのコンピュータウィルスチェック結果を管理装置に送信し、管理装置で一括管理することにより、ネットワーク下の複数の端末装置のコンピュータウィルスへの感染を容易にチェックできる等の特長を有する。請求項２０によれば、管理装置から端末装置にコンピュータウィルスチェック要求とともに、コンピュータウィルスパターンを送信することにより、全ての端末装置で、同じコンピュータウィルスパターンでコンピュータウィルスチェックを実行できる。また、管理装置のコンピュータウィルスパターンを最新のパターンに更新するだけで、全ての端末装置を最新のコンピュータウィルスパターンでウィルスチェックを行うことができる等の特長を有する。

【０１２８】請求項２１によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【０１２９】請求項２２によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１３０】請求項２３によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管

理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【０１３１】請求項２４によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１３２】請求項２５によれば、管理装置から端末装置のコンピュータウィルスチェック手段を起動するコンピュータウィルスチェック要求を複数の端末装置に送信し端末装置でコンピュータウィルスチェックを自動的に実行することにより、管理装置からの要求に応じてコンピュータウィルスチェックを行うことができるので、コンピュータウィルスの管理を所定のスケジュールにより確実に行うことができる等の特長を有する。

【０１３３】請求項２６によれば、管理装置からコンピュータウィルスチェック要求を複数の端末装置に送信し、複数の端末装置で管理装置に記憶されたコンピュータウィルスチェック手段にアクセスし、コンピュータウィルスチェックを実行することにより複数の端末装置のそれぞれにコンピュータウィルスチェック手段を必要がないので、端末装置の容量を有効に使用でき、また、管理装置のコンピュータウィルスチェック手段を最新のバージョンに設定しさえすれば、複数の端末装置の全てで同じ最新のコンピュータウィルスチェック手段でコンピュータウィルスをチェックできるので、コンピュータウィルスに対して有効に対処できる等の特長を有する。

【図面の簡単な説明】

【図１】本発明の第１実施例のシステム構成図である。

【図２】本発明の第１実施例のサーバマシンのブロック構成図である。

【図３】本発明の第１実施例のコンピュータウィルスチェック要求スケジュールのデータ構成図である。

【図４】本発明の第１実施例の集計結果累積領域のデータ構成図である。

【図５】本発明の第１実施例のクライアントマシンのブロック構成図である。

【図６】本発明の第１実施例のクライアントマシンのコンピュータウィルスチェック結果領域のデータ構成図である。

【図７】本発明の第１実施例のクライアントマシンのコンピュータウィルスパターン領域のデータ構成図である。

【図８】本発明の第１実施例のコンピュータウィルスチェック要求プログラムの処理フローチャートである。

【図９】本発明の第１実施例のクライアントマシンのコンピュータウィルスチェックプログラムの処理フローチャートである。

【図１０】本発明の第１実施例のサーバマシンのコンピュータウィルスチェック結果処理プログラムの処理フローチャートである。

【図１１】本発明の第１実施例のグループ担当者に送信するコンピュータウィルスチェック結果一覧のフォーマットである。

【図１２】本発明の第２実施例のサーバマシンのブロック構成図である。

【図１３】本発明の第２実施例のコンピュータウィルスチェック要求プログラムの処理フローチャートである。

【図１４】本発明の第３実施例のサーバマシンのブロック構成図である。

【図１５】本発明の第３実施例のクライアントマシンのブロック構成図である。

【図１６】本発明の第３実施例のクライアントマシンのコンピュータウィルスチェック制御プログラムの処理フローチャートである。

【図１７】本発明の第４実施例のサーバマシンのブロック構成図である。

【図１８】本発明の第４実施例のサーバマシンのファイル装置の発信状況管理領域のデータ構成図である。

【図１９】本発明の第４実施例のサーバマシンのコンピュータウィルスチェック要求処理の処理フローチャートである。

【符号の説明】

１　ネットワークシステム

２，１１０　サーバマシン

３－１－１～３－１－ｍ１，３－２－１～３－２－ｍ２・・・３－ｎ－１～３－ｎ－ｍｎ，１２０　クライアントマシン

１１，２１　通信制御部

１２，２２，１１１，２１１　ファイル装置

１３，２３　入出力コントローラ

１４，２４　ＣＰＵ

１５，２５　ＲＡＭ

１６，２６　ディスプレイ

１７，２７　表示コントローラ

１８，２８　キーボード

１９，２９　キーボードコントローラ

２０，３０　バス

１２ａ，２２ａ・データ領域

１２ｂ，２２ｂ，１１２・プログラム領域

１２ｃ　コンピュータウィルスチェック要求スケジュール領域

１２ｄ　集計結果累積領域

２２ｃ　コンピュータウィルスチェック結果領域

33

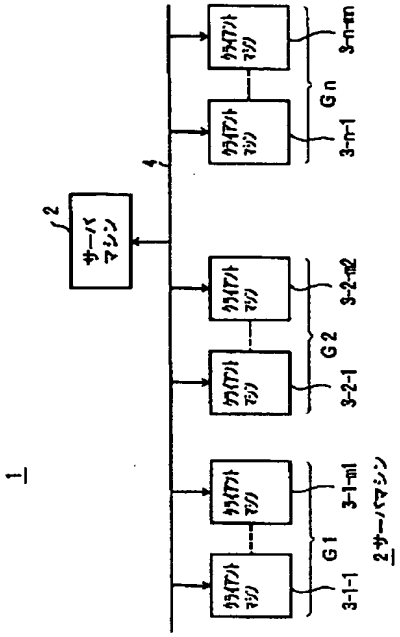
２２ｄ　コンピュータウィルスパターン領域

34

２１２　発信状況管理領域

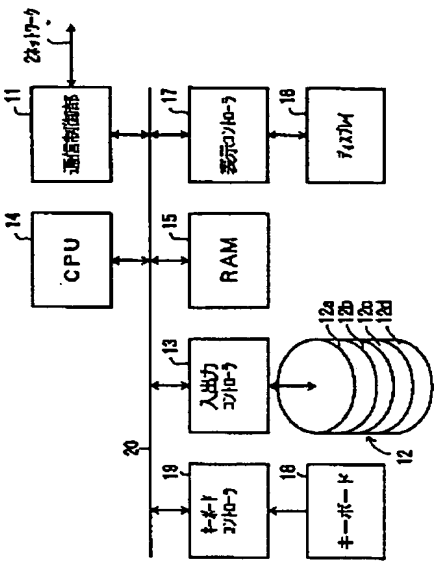
【図１】

本発明の第１実施例のシステム構成図



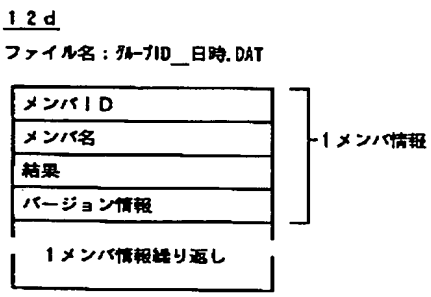

【図２】

本発明の第１実施例のサーバマシンのブロック構成図



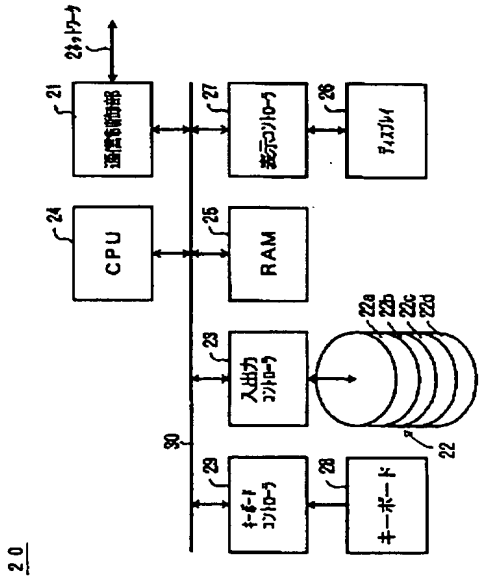

【図４】

本発明の第１実施例の集計結果累積領域のデータ構成図



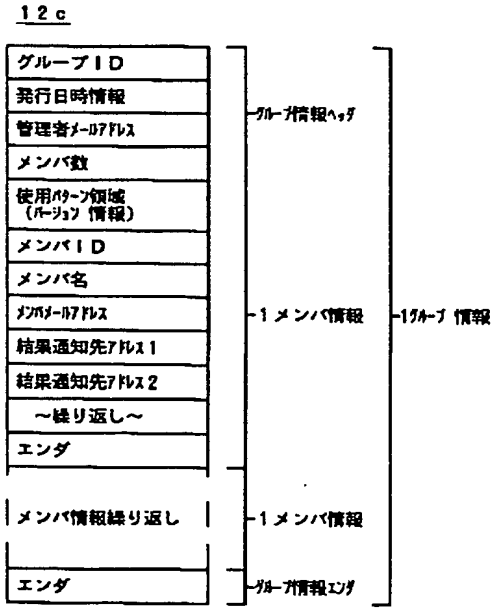

【図５】

本発明の第１実施例のクライアントマシンのブロック構成図



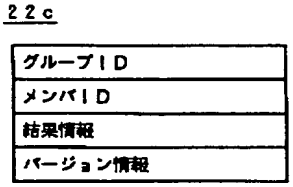

【図３】

本発明の第１実施例のコンピュータウィルスチェック要求スケジュールのデータ構成図



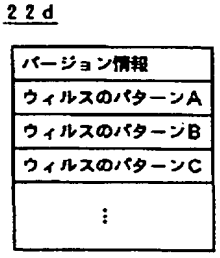
【図６】

本発明の第１実施例のクライアントマシンのコンピュータ
ウィルスチェック結果領域のデータ構成図



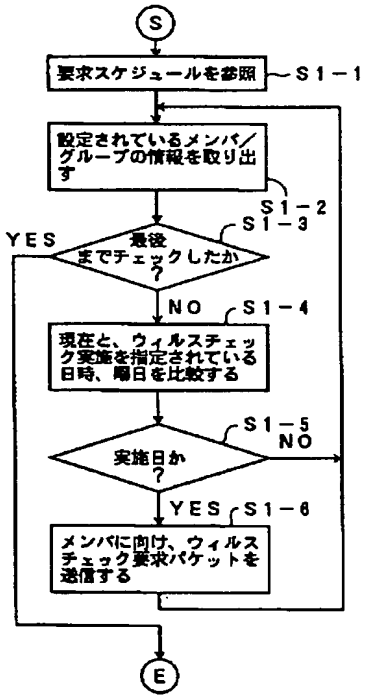

【図７】

本発明の第１実施例のクライアントマシンのコンピュータ
ウィルスパターン領域のデータ構成図



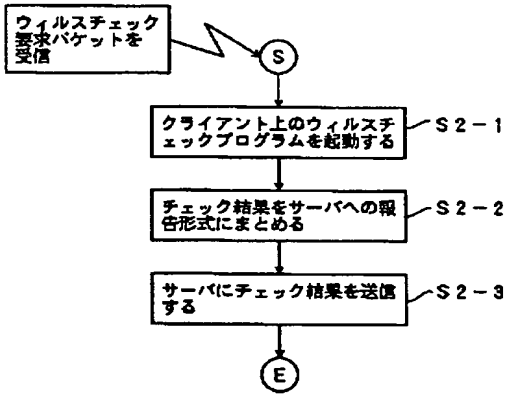

【図８】

本発明の第１実施例のコンピュータウィルスチェック
要求プログラムの処理フローチャート




【図９】

本発明の第１実施例のクライアントマシンのコンピュータ
ウィルスチェックプログラムの処理のフローチャート




【図１１】

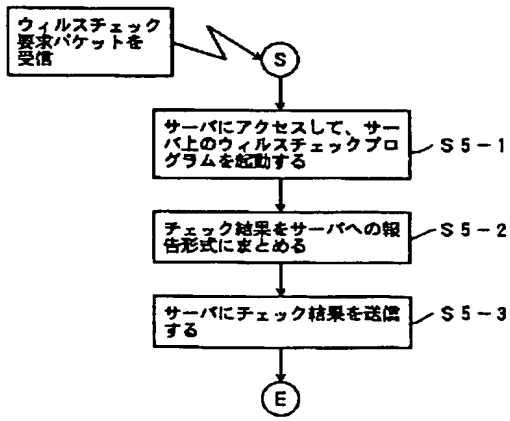
本発明の第１実施例のグループ担当者に送信するコンピュータ
ウィルスチェック結果一覧のフォーマット

テキストファイル

```
ｸﾞﾙｰﾌﾟID:A
試行日時:97/07/07
----------
[メンバ名：A氏]
使用パターン：V**L**
結果：Normal end
----------
[メンバ名：B氏]
使用パターン：V**L**
結果：ウィルス**発見／除去しました
```

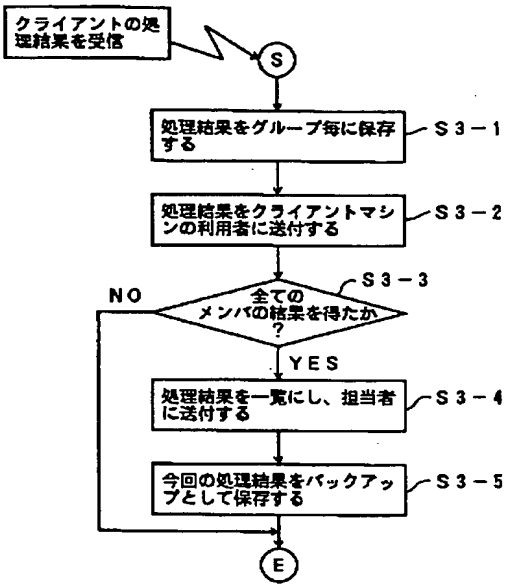
【図１６】

本発明の第３実施例のクライアントマシンのコンピュータ
ウィルスチェック制御プログラムの処理フローチャート



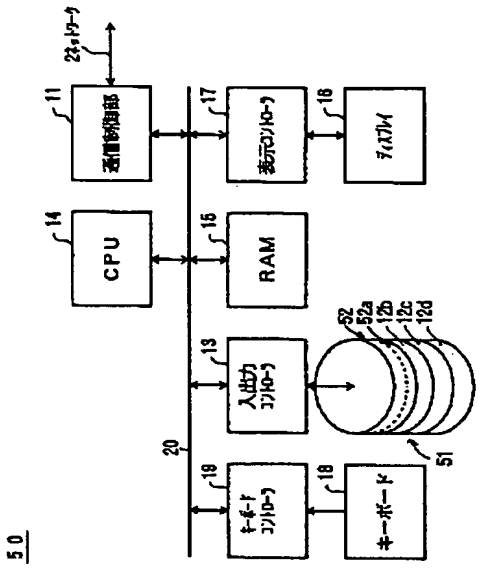
【図１０】

本発明の第１実施例のサーバマシンのコンピュータウィルスチェック結果処理プログラムの処理フローチャート



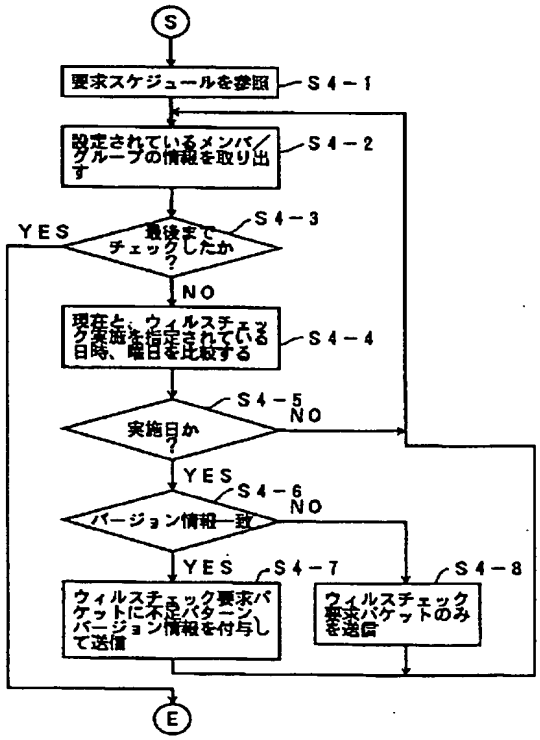

【図１２】

本発明の第２実施例のサーバマシンのブロック構成図



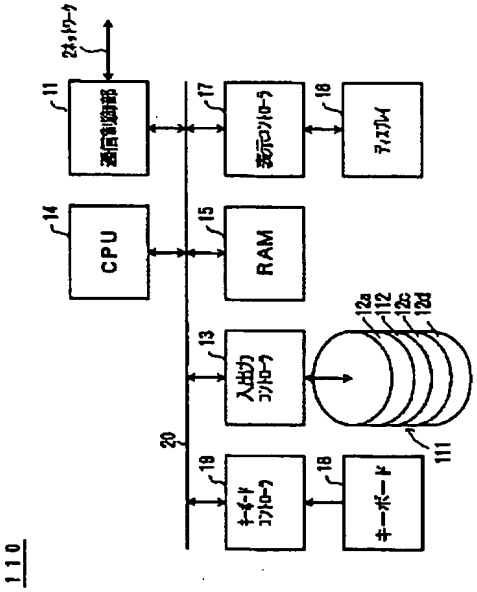

【図１３】

本発明の第２実施例のコンピュータウィルスチェック要求プログラムの処理フローチャート



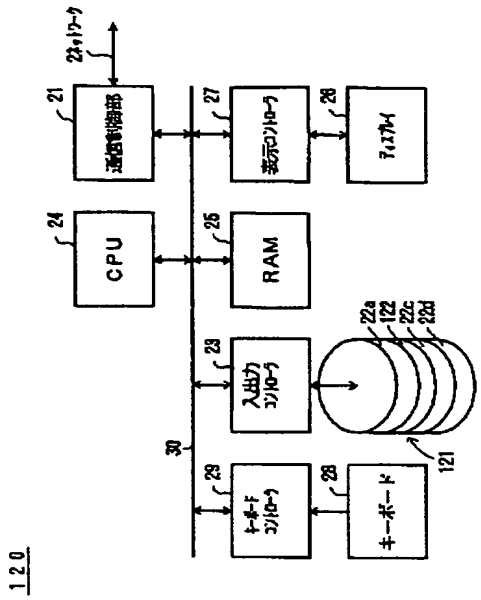

【図１４】

本発明の第３実施例のサーバマシンのブロック構成図



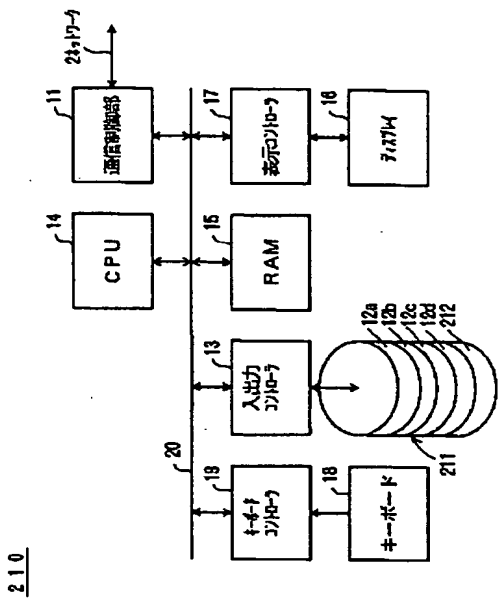
【図１５】

本発明の第３実施例のクライアントマシンのブロック構成図




【図１７】

本発明の第４実施例のサーバマシンのブロック構成図




【図１８】

本発明の第４実施例のサーバマシンのファイル装置の発信状況管理領域のデータ構成図

発信状況管理構造

| |
|---|
| グループＩＤ |
| メンバＩＤ |
| メンバメールアドレス |
| 発信予定日 |
| 発信期限 |
| 繰り返し |

１つの情報

【図１９】

本発明の第４実施例のサーバマシンのコンピュータウィルスチェック要求処理の処理フローチャート